TENNESSEE DEPARTMENT OF FINANCE AND ADMINISTRATION
Enterprise Security Officer

Job Summary: Reports to the Chief Information Security Officer (CISO) within Strategic Technology Solutions, the Enterprise Security Officer is responsible for assisting the CISO with developing, implementing and directing a comprehensive information technology security and compliance program. This position is responsible for the development of policies, providing executive guidance within IT risk management and the overall security posture of the organization, as well as promoting security awareness and ensuring compliance with statutory and regulatory requirements regarding information access and security.

Responsibilities:

- Provide recommendations to the CISO on information security standards and best practices for IT projects.
- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls.
- Promote policy, compliance, roles and responsibilities to the Business and IT shops.
- Deliver security and compliance awareness training.
- Oversee the development, implementation, and maintenance of the statewide security policy, enterprise security standards, guidelines, and methodologies.
- Initiate, drive, and control security projects to enhance technical security infrastructure and organizational security within the state.
- Assist with the development and implementation of the Information Security Awareness training program to provide awareness and ensure compliance within the state.
- Audit and validate against Federal/State policies and regulations.
- Promote awareness of current policies and standards, as well as revisions and developments on an ongoing basis.
- Act as an advisor and provide consistent interpretation of security policies to technology teams and business owners statewide.
- Educate and explain technical security controls as they apply to compliance.
- Review the security program execution and make appropriate adjustments/recommendations to resolve issues on a continuous basis.
- Provide recommendations on cloud security solutions to include development, implementation and management of the organization’s security vision, strategy and security programs.
- Discuss compliance and audit issues with management and develop action plans to address them.
- Prepare, document, maintain and disseminate information security policies, standards and methodologies.
- Ensure that information security audits are conducted on a regular basis.
- Assist business owners with creating and developing remediation plans for any identified regulatory gaps or deficiencies.
- Interface with law enforcement agencies and other government agencies to address security lapses and to ensure that the organization maintains a strong security posture.
- Respond appropriately with resources and information to requests submitted by internal and external auditing functions.
- Communicate directly with regulatory authorities.
- Maintain relationships with local, state and federal law enforcement and other related government agencies.
- Maintain relationships with agencies and boards to establish and facilitate security and risk management processes, including the reporting and oversight of remediation efforts to address negative findings; identifies acceptable levels of risk; and establishes roles and responsibilities with regards to information compliance and protection.

Minimum Qualifications: Bachelor’s degree in an IT or Business related field. Relevant professional information technology experience may be substituted for the required degree.

- Eight years of experience in information technology, information security or risk management.
- Knowledge of information security standards and best practices.
- Knowledge of federal, state, and local laws, rules, regulations, policies and procedures, and best practices as they relate to information systems governance.
- Knowledge of regulatory guidance in security and risk management.
- Knowledge of Risk/Audit/Compliance competencies especially as it relates to security and risk management.

- Knowledge of technological trends and developments in the area of information security, governance, risk and compliance management, and data loss prevention.
- Knowledge of management of an effective security and compliance program, including training, monitoring, conducting and documenting investigations, addressing violations, and monitoring corrective actions.
- Knowledge of Governance, Risk and Compliance tools.
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security and risk-related concepts to technical and non-technical audiences.

Preferred Qualifications:

- Prior state government experience is a plus.

Knowledge, Skills, Abilities, Competencies:

- Decision Quality
- Business Acumen
- Problem Solving
- Customer Focus
- Innovation Management
- Priority Setting
- Drive for Results
- Conflict Management

The State of TN is an Equal Opportunity Employer.

Resumes should be submitted via email to EIT.Resumes@tn.gov

Pursuant to the State of Tennessee's Workplace Discrimination and Harassment policy, the State is firmly committed to the principle of fair and equal employment opportunities for its citizens and strives to protect the rights and opportunities of all people to seek, obtain, and hold employment without being subjected to illegal discrimination and harassment in the workplace. It is the State's policy to provide an environment free of discrimination and harassment of an individual because of that person's race, color, national origin, age (40 and over), sex, pregnancy, religion, creed, disability, veteran's status or any other category protected by state and/or federal civil rights laws.